

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,005	04/12/2001	Douglas A. Hardy	GE04591	9509

7590 07/30/2004

Stanley A. Schlitter
JENNER & BLOCK, LLC
One IBM Plaza
Chicago, IL 60611

EXAMINER

SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 07/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/833,005

Applicant(s)

HARDY ET AL.

Examiner

Eleni A Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 January 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>7/19/2004</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, and 2 are rejected under 35 U.S.C. 102(e) as being anticipated by Arnold (U.S. Patent 5,956,408).

4. As per claim 1, Arnold teaches a method for enabling encryption and decryption of an initial version of a software product comprising the steps of:

generating a first encryption key (Col. 6 lines 66-col. 7 lines 8, Fig. 3 No. 100);

encrypting the initial version of the software product with said first

encryption key to generate an encrypted initial software product (Col. 7 lines 15-21, Fig. 3 No. 120);

generating a first key portion of said first encryption key (Col. 6 lines 66-col. 7 lines 7);

calculating a second key portion by utilizing said first key portion and said

Art Unit: 2136

first encryption key to generate a said second key portion such that the combination of said first key portion and second key portion form said first encryption key (Col. 6 lines 66-col. 7 lines 15);

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product (Col. 7 lines 21-col. 7 lines 44, Fig. 3 No. 130-180);

combining said first key portion and said second key portion to provide said first encryption key in said hardware product (Col. 7 lines 21-col. 7 lines 44, Fig. 3 No. 130-180); and

utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product (Col. 7 lines 66-col. 8 lines 11).

5. As per claim 2, Arnold teaches the method wherein said step of generating a first encryption key utilizes a random number generator to generate said first encryption key (Col. 7 lines 55-col. 7 lines 60).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. Patent 5,956,408) in view of Applicant Admitted Prior Art (AAPA), and in further view of Masuda et al. (Masuda, U.S. Patent No.: 6,714,649 B1)

8. As per claim 3, Arnold teaches all the subject matter as described above.

Arnold do not explicitly teach an "exclusive or" logic operation;

AAPA teaches an "exclusive or" logic operation (Page 4 lines 8-29)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the applicant's teaching and apply "exclusive or" in the system of providing encryption key because it would it would combine SPLIT A and TOKEN to form KEY A. (page 4 lines 8-29)

Arnold and AAPA do not explicitly teach combining the first key portion and said first encryption key to calculate said second key portion.

However Masuda teaches combining the first key portion and said first encryption key to calculate said second key portion. (Col. 2 lines 15-46)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Masuda with in the system of Arnold and AAPA because it would generate a second key-encrypted scramble key by encrypting the scramble key with a second key different from the first key and update the first key to enhance security and perform update efficiently (Abstract).

9. As per claim 4, Arnold teaches the method wherein said step of combining said first key portion and said second key portion to combine said first key portion and said second key portion to provide said first encryption key (Col.7 lines 21-35);

AAPA teaches an "exclusive or" logic operation (Page 4 lines 8-29) The rationale for combining are the same as claim 3 above.

10. Claims 5-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (U.S. Patent 5,956,408) in view of Applicant Admitted Prior Art (AAPA), and Masuda et al. (Masuda, U.S. Patent No.: 6,714,649 B1), and in further view of Leppek (U.S. Patent No. 5,933,501)

11. As per claim 5, Arnold, AAPA, and Masuda teach all the subject matter as described above.

Arnold teaches the method further enabling an update of said first encryption key to provide a second encryption key to secure a different version of the initial software product (Claim 1, col. 4 lines 42-51, col. 6 lines 31-37), further comprising the steps of:

installing said third key portion (Col. 7 lines 1-3) and the encrypted different version of the software product in said hardware product (Col. 4 lines 43-51, col. 7 lines 16-27);

using the encryption key to decrypt the encrypted different version of the software product (Col. 8 lines 4-11, Fig. 5 No. 280)

Arnold and AAPA fail to explicitly teach the generating the second encryption key;
encrypting the different version of the initial software product with the second encryption key to provide an encrypted different version of the software product;
combining the first encryption key and the second encryption key to provide

a third key portion;

combining said third key portion and said second key portion to generate a fourth key portion in said hardware product; and

combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product;

However Masuda teaches generating the second encryption key (Col. 2 lines 15-46); encrypting the different version of the initial software product with the second encryption key to provide an encrypted different version of the software product (Col. 3 lines 33-47);

combining the first encryption key and the second encryption key to provide a third key portion (Col. 2 lines 13-47) The rationale for combining are the same bases are claim 3 above;

Arnold, AAPA, and Masuda do not explicitly teach combining said third key portion and said second key portion to generate a fourth key portion in said hardware product;

combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product;

However Leppek teaches the virtual encryption scheme, and the order of the encryptors within the sequence to which the data is applied may vary as desired (Col. 2 lines 49-55); this reads on combining said third key portion and said second key portion to generate a fourth key portion in said hardware product;

combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product (Claim 1 (b), Col. 2 lines 49-55, col. 3 lines 48-59);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Leppek with in the system of Arnold, AAPA,

and Masuda because it would enable a computer end user to securely encrypt data communications in such a manner that effectively prevents a usurper from decrypting the data (Col. 1 lines 5-12).

12. As per claim 6, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition Arnold teaches the method wherein said step of providing said second encryption key utilizes a random number generator to generate said second encryption key (Col. 7 lines 55-60).

13. As per claim 7, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, AAPA teaches utilizes an "exclusive or" logic operation (Page 4 lines 8-29) The rational for combining are the same as claim 3 above;

Masuda teaches the method wherein said step of combining the first encryption key and the second encryption key to combine said first encryption key and said second encryption key to generate said third key portion (Col. 2 lines 13-47) The rational for combining are the same bases are claim 3 above;

14. As per claim 8, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, AAPA teaches utilizes an "exclusive or" logic operation (Page 4 lines 8-29) The rational for combining are the same as claim 3 above;

Leppek teaches the method wherein said step of providing said second encryption key to combine said first key portion and said fourth key portion to provide said second encryption key (Col. 2 lines 49-55, col. 3 lines 48-59) The rational for combining are the same as claim 5 above.

15. As per claim 9, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Leppek teaches the method wherein said initial version of software product and said different version of said initial version of said software product are non-sequential versions (Col. 2 lines 49-55, col. 3 lines 48-59) The rational for combining are the same as claim 5 above.

16. As per claim 10, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Leppek teaches the method wherein said second encryption key is non-sequential with said first encryption key (Col. 2 lines 49-55, col. 3 lines 48-59) The rational for combining are the same as claim 5 above.

17. As per claim 11, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Arnold teaches a method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided by a provider to a user of a hardware product, (Col. 7 lines 1-7, col. 6 lines 31-37) said method comprising:

providing a first encryption key (Col. 6 lines 31-37, col. 7 lines 21-27);

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (Col. 7 lines 15-21, Fig. 3 No. 120);

providing a first key portion (Col. 6 lines 31-37);

storing said first key portion in storage means external to the hardware (Col. 7 lines 21-27);

storing said second key portion separately from said first key portion in a tamper proof memory means in the hardware product (Col. 4 lines 1-14);

storing said encrypted software product in a further memory means in the hardware product (Col. 7 lines 21-27);

combining said first key portion and said second key portion in the hardware product to provide said first encryption key (Col. 10 lines 66-col. 11 lines 2);

decrypting said encrypted initial software product with said first encryption key (Col. 7 lines 21-36);

Arnold does not explicitly teach calculating a second key portion to form said first encryption key;

However Masuda teaches utilizing said first key portion and said first encryption key to calculate a second key portion such that the combination of said first and second key portions form said first encryption key (Col. 2 lines 15-46) The rationale for combining are the same as claim 3 above.

18. As per claim 12, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Arnold teaches the method wherein said step of providing a first encryption key utilizes a random number generator to generate said first encryption key (Col. 7 lines 55-60).

19. As per claim 13, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, AAPA teaches utilizing and "exclusive or" logic operator (Page 4 lines 8-29) The rationale for combining are the same as claim 3 above;

Art Unit: 2136

Masuda teaches the method wherein said step of utilizing said first key portion and said first encryption key to calculate said second key portion (Col. 2 lines 15-46) The rational for combining are the same as claim 3 above.

20. As per claim 14, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Arnold teaches the method wherein said step of combining said first key portion and said second key portion performed by said hardware product (Col. 7 lines 21-27).

AAPA utilizing an "exclusive or" logic operation (Page 4 lines 8-29) The rational for combining are the same as claim 3 above;

21. As per claim 15, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Arnold teaches the method further enabling security of an update of said first encryption key and providing a second encryption key for encrypting a different version of the initial software product (Col. 10 lines 66-col. 11 lines 2), further comprising:

installing said third key portion in said tamper proof memory means (Col. 4 lines 1-14, col. 10 lines 66-col. 11 lines 2);

installing said encrypted different version (Col. 4 lines 43-51) of the initial software product in said further memory means in the hardware product (Abstract, Col. 4 lines 43-51);

using said encryption key in the hardware product to decrypt the encrypted different version of the initial software product (Col. 8 lines 4-11, Fig. 5 No. 280)

Masuda teaches

generating the second encryption key (Col. 2 lines 15-46);

encrypting the different version of the initial software product with said second encryption key to provide an encrypted different version of the initial software product (Col. 3 lines 33-47) The rational for combining are the same as claim 3 above;

Leppek teaches

combining said third key portion and said second key portion to generate a fourth key portion in the hardware product (Col.2 lines 47-55);

combining said first encryption key and said second encryption key to provide a third key portion (Col.3 lines 47-59);

combining said first key portion and said fourth key portion to provide said second encryption key in the hardware product (Col.3 lines 47-59)The rational for combining are the same bases as claim 5 above.

22. As per claim 16, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Arnold teaches the method wherein said step of generating a second encryption key utilizes a random number generator (Col. 7 lines 55-60).

23. As per claim 17, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, AAPA teaches an "exclusive or" logic operation (Col. 4 lines 8-29);

Masuda teaches the method wherein said step of combining said first encryption key and said second encryption key to generate a third key portion (Abstract) The rational for combining are the same as claim 3 above.

Art Unit: 2136

24. As per claim 18, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, AAPA teaches an "exclusive or" logic operation (Col. 4 lines 8-29);

Leppek teaches the method wherein said step of combining said first key portion and the fourth key portion to provide said second encryption key (Col. 2 lines 49-55, Col. 3 lines 48-59) The rational for combining are the same bases as claim 5 above.

25. As per claim 19, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Leppek teaches the method wherein said initial version of a software product is non-sequential with said different version of the initial software product (Col. 2 lines 49-55, Col. 3 lines 48-59) The rational for combining are the same bases as claim 5 above.

26. As per claim 20, Arnold, AAPA, Masuda, and Leppek teach all the subject matter as described above. In addition, Leppek teaches the method wherein said second encryption key is non-sequential with said first encryption key (Col. 2 lines 49-55, Col. 3 lines 48-59) The rational for combining are the same bases as claim 5 above.


27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

Art Unit: 2136

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100